VERITAS™

Veritas NetBackup SaaS Protection

Annex 1

Data Exporter
The Data Exporter is:

Customer and those of its Affiliates that are contractually permitted to use the Veritas service known as NetBackup SaaS Protection (“Service”)

Data Importer
The data importer is:

Veritas Technologies, LLC as the provider of the Service, either in its own right where the Customer has contracted directly with the Data Importer, or as subcontractor to Veritas Storage (Ireland) Limited.

Data subjects
The Personal Data transferred concern the following categories of data subjects (please specify):

Any individual whose personal data appears in the Data Exporters files.

In the context of “follow the sun” support: Workers of the Data Exporter that are named as persons authorised to contact Veritas for support

Categories of data

As determined by the Data Exporter, all categories of personal data may be processed. Common elements of personal data contained in the user files include but are not limited to, user names, file names, metadata and system logs and further identifiable information. Further personal data my include Login credentials; and/or backup information, including metadata, files folders, notes and tasks.

In the context of “follow the sun” support: name, email name, email address, company name and address, job title, contact number and any data disclosed on behalf of Data Exporter

Special categories of data (if appropriate)
The Personal Data transferred concern the following special categories of data (please specify):

N/A

Processing operations
The metadata are processed to enable the Data Exporter for the purposes of backup and recovery of SaaS applications. The processing of Personal Data contained within the metadata is incidental to the purposes of the processing.

In the context of “follow the sun” support: employee/worker contact details are used to verify that the person contacting Veritas for support is the employee/worker of Data Exporter and therefore authorised to seek support on Data Exporters’ behalf.

Subprocessors
To view a list of current sub-processors which may have access to personal data processed by the Service, please visit: https://www.veritas.com/content/dam/Veritas/docs/policies/sub-processors-for-veritas-services.pdf

For information regarding any historical sub-processors related to your use of the Service, please contact privacy@veritas.com

Veritas NetBackup SaaS Protection

Annex 2
Security Measures

1. **Access control to premises and facilities**
   Measures must be taken to prevent unauthorized physical access to premises and facilities holding personal data. Measures shall include:

   - Access control system
   - ID reader, magnetic card, chip card

   - (Issue) of keys
   - Door locking (electric door openers, etc.)
   - Surveillance facilities
   - Alarm system, video/CCTV monitors
   - Logging facility exits/entries

2. **Access control to systems**
   Measures must be taken to prevent unauthorized access to IT systems. These must include the following technical and organizational measures for user identification and authentication:

   - Password procedures (including special characters, minimum length, forced change of password)
   - No access for guest users of anonymous accounts
   - Central management of system access
   - Access to IT systems subject to approval from HR management and IT system administrators

3. **Access control to data**
   Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorized (input, reading, copying, removal) modification or disclosure of data. These measures shall include:

   - Differentiated access rights
   - Access rights defined according to duties
   - Automated log of user access via IT systems
   - Measures to prevent the use of automated data-processing systems by unauthorized persons using data communication equipment

4. **Disclosure control**
   Measures must be taken to prevent the unauthorized access, alteration or removal of data during transfer.

5. **Input control**
   Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted and by whom must be maintained. Measures should include:

   - Logging user activities on IT systems
   - Ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment

6. **Job control**
   Measures should be put in place to ensure that data is processed strictly in compliance with the data importer’s instructions. These measures must include:

   - Unambiguous wording of contractual instructions

7. Availability control

Measures should be put in place to ensure that data are protected against accidental destruction or loss. These measurements must include:

- Ensuring that installed systems may, in the case of interruption, be restored
- Ensure systems are functioning, and that faults are reported
- Ensure stored personal data cannot be corrupted by means of a malfunctioning of the system
- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Remote storage
- Firewall and intrusion detection systems

8. Segregation control

Measures should be put in place to allow data collected for different purposes to be processed separately. These should include:

- Restriction of access to data stored for different purposes according to employee duties
- Segregation of business IT systems
- Segregation of IT testing and production environments